Getting the Best Outcomes

Pathways for Data Protection and Privacy Authorities

September 2024

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Richard Thomas
CBE LLD

Table of Contents

Table of Contents (continued)

Foreword

At a time of unprecedented digitalisation of our societies and economies, driven by data and transformative technologies, privacy and data protection authorities (DPAs) are becoming a key digital regulator, and their role is central to the progress. DPAs are facing growing demands to enable responsible and trusted use of personal data, consider competing interests and fundamental rights and collaborate with other digital regulators at the intersection of overlapping digital rules.

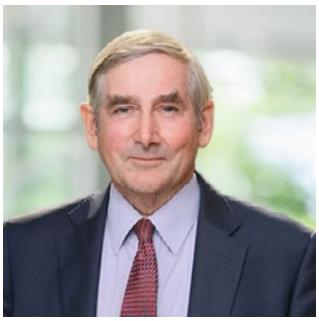
This raises two fundamental questions for DPAs - What should DPAs be doing and prioritising? How should they be doing it? Yet, there is surprisingly little discussion about the outcomes that DPAs should seek or the best ways to secure them.

These are not easy questions, but they are essential, especially in shaping regulators' strategies and priorities and their risk-based approach to supervision and enforcement. When resources are scarce, and expectations are high, it is all the more important to focus on what the right outcomes are and how best to deliver them for people and society. There is plenty of aspirational language, but perhaps too many unchallenged assumptions and too much focus on "tick-box" compliance with procedural requirements. This can cause a loss of focus on what both DPAs and the regulated community should be aiming to achieve and how best to achieve those goals.

This paper is unashamedly pragmatic. It draws on experience in other sectors of regulation and on evidence as to what does —and does not—work. It offers Pathways to Effectiveness—primarily to stimulate discussion. We are not putting forward a detailed blueprint. But we are hoping that DPAs and accountable regulated organisations alike will give serious consideration to our suggestions in the interest of getting the best outcomes at a time of profound digital industrial revolution.

Bojana Bellamy

President
CIPL



Richard Thomas CBE

Strategy Adviser
CIPL and UK Information Commissioner (2002–2009)

I. Introduction and Summary

The aim of this White Paper is to set out ways for Data Protection Authorities (DPAs) to maximise their effectiveness as regulatory bodies in a time of growing demand for their time and expertise[1]. It builds on CIPL's previous work and 2017 Paper "Regulating for Results".[2]

This is a difficult and potentially controversial undertaking. There is no consensus as to what an "effective" DPA looks like, or even what overall outcomes are sought. CIPL, of course, does not wish to tell DPAs how to do their job. Instead, we have set out some ideas based on our experience and research, which we hope will be helpful to policymakers and lawmakers who are legislating in relation to the powers and roles of DPAs in the new digital society and to DPAs themselves.

The paper is divided into seven sections, each of which concludes with "Key Messages" with the aim to keep it as short and accessible as possible.

Following the introduction, Section II summarises studies that document the limitations of traditional approaches to regulation in other social and economic sectors and sets out alternative approaches that are proving to be successful in other regulatory areas. Focus is placed on Responsive Regulation (Regulatory Delivery) and on the Outcome-Based Regulation model. The central message is that sanctions play a limited role in deterring and changing behaviours and that effective regulators focus on improving behaviours, with choices of intervention guided by the segmentation of those they regulate along a "Sinner/Saint" spectrum.

Section III looks at the challenges in applying the learnings from other regulatory areas to data protection. Data Protection is special in that the law impacts horizontally on all sectors. It is complex and focuses on procedural compliance, yet includes aspirational principles such as fair processing and transparency. Outside of general terms, data protection laws do not usually give DPAs clear objectives or priorities, with new regulatory areas such as AI adding to the challenge. Ultimately, DPAs have too many functions and are often under-resourced.[3]

Section IV sets out the core thinking for DPAs. We argue that clarity and consensus about the **outcome(s) that are sought are fundamental** but are currently missing. Although there are many possibilities, we suggest that the core Outcome could be:

> **Facilitating the free flow of data while ensuring that individuals can trust that they will not be significantly harmed by invasions of their privacy or misuse of their personal information.**

Whatever is adopted, a clear outcome is necessary to guide the setting of **Objectives** for a DPA and its **Priorities**. Although we have made some suggestions, it is for each DPA—in line with the relevant legislation—to articulate the Outcome(s) it seeks to secure and the objectives to bring that about.

1 Although this Paper uses the language of Data Protection and Data Protection Authorities, our messages are aimed equally at those jurisdictions which use the language of Privacy.

2 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf

3 European Data Protection Board, Contribution of the EDPB to the report on the application of the GDPR under Article 97 – 2023, according to the report: "The vast majority of SAs have explicitly stated that they do not have enough resources while there are few SAs who do not see a need for further resources at this stage", p. 32.

Building on our 2017 paper, Regulating for Results, we divide the functions of DPAs into three main groups:

The **Leader** role—using the expertise, authority and influence of the DPA to educate, incentivise, and change behaviour—should have top priority.

The **Police Officer** role—taking enforcement action—should be ranked in second place.

The **Ombudsman** role—handling complaints from individuals—should have the lowest priority.

The Leadership role (leading, educating and engaging) is fundamental to promoting responsible data use and facilitating prosperity and innovation. It should have top priority. The Ombudsman's role (resolving individual complaints) is resource-hungry and often unproductive and should have the lowest priority. The Police Officer role will be most beneficial against those whose offending behaviour is deliberate, repetitive or otherwise seriously unacceptable.

The Key Messages at the end of each section are highlighted at the end of this Introduction. They can be distilled into a single set of **Pathways to Effectiveness**:

PATHWAYS TO EFFECTIVENESS

- **Priorities** are essential. Currently, DPAs have too many functions, are often seriously under-resourced and are unable to fulfil all their duties.
- In setting priorities, DPAs have to be **"Selective to be Effective"**. They should adopt a Risk-Based Approach to all their functions—supervision, guidance and enforcement.
- DPAs should prioritise **Leadership** by promoting the responsible use of personal information and helping organisations get it right.
- Fines resulting from enforcement action need to be one of the tools in a DPA's toolkit. However, evidence suggests that fines *a priori* or alone do little to significantly alter behaviour or contribute much to declared Outcomes.
- Where a sanction is warranted, **Enforcement Orders** requiring a change in behaviour will usually be a more effective remedy.
- The **complaint-handling** function is not an efficient use of scarce resources and will not contribute directly to overall effectiveness.
- DPAs should use complaints as an important source of intelligence, but as far as possible, aim to restrict detailed investigations to cases of strategic value and explore other avenues such as amicable settlement procedures and referring complaints in the first instance to the controllers and processors concerned.
- DPAs should **define KPIs** to measure their success—the size or number of fines is not an appropriate measure.
- DPAs should strive to **coordinate** their approach through relevant cooperation bodies to limit fragmentation.[4] This also includes working with other digital and data regulators in a more formalised and institutionalised manner.
- **Guidance** must be risk-based, authoritative, usable, in plain language and targeted to identified audiences.
- **Constructive engagement between DPAs and regulated entities** is an important tool for achieving common goals of responsible data handling. This is even more important given the complexities of transformative technologies and broader digital transformation of our societies and economies.
- **DPAs should strive to help those who want to get it right while being tough on those who do not. Specifically, DPAs should support and encourage organisational accountability,** especially given its potential to deliver and demonstrate effective and risk-based data protection and responsible use of data in practice.

4 e.g. EDPB, APPA, GPA, Ibero-American Network

Sources and Feedback

Aiming to be easily readable, we have kept messages and discussions as succinct as possible. A fuller analysis of the issues can be found in **Regulating for Results**[5], the discussion paper which CIPL published in 2017.

This White Paper can be seen as an updated summary. It has benefited substantially from feedback on that discussion paper. It was discussed at the conference of the Global Privacy Assembly in Hong Kong in 2017, at seminars in London, Brussels, Washington and Oxford and during two virtual events with DPAs and stakeholders. Most significantly, CIPL was then invited to preview this Paper at the closed plenary session of the Global Privacy Assembly's conference in Istanbul in October 2022. It—and presentations from other sectors—stimulated considerable discussion on that occasion and appeared to be well-received.[6]

The subject-matter of this paper—especially the focus on the need for Outcome-based regulation—was also discussed extensively at CIPL's Executive Retreat in Madrid in March 2024.

Since then, a **Global Review of Data Protection Authority Strategies**[7] has been independently published (in April 2024) by Steve Wood, Marie-Charlotte Roques-Bonnet and Sebastian Page. Although focused on current practice, its conclusions are largely consistent with this White Paper. It is further referenced in Section III on Outcomes, Objectives and Priorities.

Finally, this paper also takes into consideration findings from the 2024 report of the Fundamental Rights Agency "GDPR in Practice—Experiences of Data Protection Authorities".[8]

KEY MESSAGES FROM OTHER SECTORS

- Conventional approaches—adversarial enforcement—have limited effectiveness for changing long-term behaviour within organisations.
- Sanctions are rarely an active deterrent.
- Effective regulators adopt a risk-based approach and focus on behaviours, with choices of intervention guided by segmenting those they regulate.
- Clarity about the desired outcomes is essential.
- Open and constructive engagement, where regulators support trusted regulatees, brings the most benefits.
- Robust penalties should be reserved for deliberate, repeated or wilful wrongdoing.

DATA PROTECTION IS SPECIAL: KEY MESSAGES

- The law impacts horizontally on all sectors.
- The law is complex and focuses on procedural compliance.
- There is no settled consensus as to the desired outcomes.
- Laws do not usually give DPAs clear objectives or priorities.
- DPAs have too many functions.
- They are under-resourced.
- Modest fees payable by regulated organisations could considerably increase overall resources.

5 https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_final_draft_-_regulating_for_results_-_strategies_and_priorities_for_leadership_and_engagement_2_.pdf

6 Centre for Information Policy Leadership, What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework; Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions.

7 Available here or a copy can be requested via team@dpa-strategy.org.

8 European Union Agency for Fundamental Rights, *GDPR in practice – Experiences of data protection authorities*

OUTCOMES, OBJECTIVES AND PRIORITIES: KEY MESSAGES

- A clear outcome is essential to guide a DPA's objectives and priorities.
- A promising outcome would be to **"Facilitate the free flow of data while ensuring that individuals can trust that they will not be significantly harmed by invasions of their privacy or misuse of their personal information"**.
- Objectives should be ambitious but as concrete and achievable as possible.
- Priorities are essential. DPAs have too many functions and cannot do everything.
- In setting priorities, DPAs have to be **"Selective to be Effective"**. This means adopting a rigorous risk-based approach in all the activities, from supervision and guidance to regulation, supervision and enforcement, to focus on areas where there is a real likelihood and severity of harm to individuals. This is fundamental if DPAs are to maximise their effectiveness
- The **Leader** role—emphasising the expertise, authority and influence of the DPA—should have top priority.
- The **Police Officer** role—taking enforcement action—should be ranked in second place.
- The **Ombudsman** role—handling complaints from individuals—should have the lowest priority.

LEADERSHIP, EDUCATION AND ENGAGEMENT: KEY MESSAGES

- The Leadership role should be the top strategic priority for a DPA
- Promoting good practice—through the expertise and authority of the DPA—incentivises and supports improved performance.
- Guidance must be authoritative, usable, in plain language and targeted to identified audiences.
- Codes of Practice, certification & seal schemes, and audits can help organisations get it right.
- Constructive engagement with regulatees is the best way to achieve common goals of responsible data handling and make a practical reality of data protection.
- Many activities can be adopted by DPAs wishing to engage constructively.
- Mutual trust—established through segmentation techniques—is an essential component.

POLICING AND ENFORCEMENT: KEY MESSAGES

- The availability of a meaningful "stick" is important for the credibility and authority of a DPA.
- But enforcement should not be seen as a first resort.
- Fines are not an indicator of success.
- The Police Officer's role and sanctions will be most beneficial against those who have failed to earn trust and whose offending behaviour is deliberate or otherwise unacceptable.
- Enforcement Orders to change behaviour will usually be a preferable remedy.

COMPLAINT-HANDLING: KEY MESSAGES

- Complaint handling is demand-led and very resource-intensive;
- It is unusual for a regulatory body also to handle complaints;
- However well handled, complaints are unlikely to contribute to effectiveness;
- This Ombudsman function should have low priority and be tightly managed to avoid the DPA being swamped;
- Complaints should be treated primarily as a source of intelligence;
- Triage and other mechanisms should be adopted to restrict investigations to cases likely to be s trategically valuable.
- DPAs should explore creating a satellite Ombudsman body to handle complaints or out-sourcing to an existing ADR-type service.

II. Regulatory Effectiveness: Conventional and Modern Approaches

1. Effective Regulation

The challenge of effectiveness is to get the best results from whatever resources are available. Many significant studies of regulatory effectiveness have emerged in recent years (see Annex 1 and Bibliography), which include findings of behavioural psychology and analysis of economic and cultural incentives for complying (or not complying) with the law. Unfortunately, however, such studies have largely bypassed discussion on effective regulation, supervision and enforcement in data protection.

This section summarises problems with conventional approaches to regulation and points to alternative approaches that have proved successful in other regulatory areas.

2. Conventional approaches to regulation

Enforcement is commonly seen as the consequence of a breach of a legal rule. A sanction is largely based on the theory that it will **deter** others from committing breaches in the future. Fear of adverse consequences prevents future wrongdoing. In simple terms, the accepted view has been that perfectly written rules lead to behaviours which are determined by the rules to achieve the "right" results in case of full compliance.

However, this concept of enforcement and deterrence is misleading and increasingly being questioned. The approach adopts a fear-based, authoritarian model of controlling behaviour and assumes that organisations will be fearful but act rationally. Rules, however, are often imperfect, encourage "gaming" by regulatees and can be subverted. More significantly, compliance with rules does not necessarily equate to satisfactory outcomes.

Assumptions of rationality contrast sharply with scientific and empirical evidence about how organisations (or the people within them) actually behave, what motivates them and what mechanisms are more effective than fear, cost calculation and deterrence. In his seminal book, Law and Corporate Behaviour[9], Prof Christopher Hodges (then Professor of Justice Systems at the University of Oxford) has drawn together some 800 pages of evidence and analysis to inform discussion about effective regulation. In the words of its sub-title, it is about "Integrating theories of regulation, enforcement, compliance and ethics".

Hodges and others[10] have criticised the theory of deterrence on several grounds:

1. Extensive empirical evidence shows the lack of effectiveness of deterrence in a wide range of practical situations.
2. The theory is linear in the sense that it assumes *historic* breaches of a rule will be identified and sanctioned and thus change *future* behaviour.

9 An abbreviated summary of key points is available here.

10 Other accessible texts are F. Blanc, *From Chasing Violations to Managing Risks* (Edward Elgar, 2018); Y Feldman, *The Law of Good People* (Cambridge, 2018); B van Rooij & A Fine, *The Behavioral Code* (Beacon Press, 2021); TR Tyler, *Advanced Introduction to Law and Psychology* (Edward Elgar, 2022).

3. The behaviours of organisations and the individuals within them are complex. Behavioural science research has established that mechanisms for acting in particular ways are frequently neither rational nor involve any cost-benefit analysis.
4. Studies of major wrongdoing and disasters consistently show that those involved paid little attention to the threat of sanctions.
5. Businesses may treat fines as a 'cost of business' rather than pursue improved behaviour.
6. Deterrence can have negative consequences and create adversarial relationships.
7. Continuous investigations and threats of sanctions militate against learning and improved performance, especially in innovative environments.
8. At best, "compliance" motivates a baseline requirement and does nothing to incentivise (and may impede) higher levels of performance and accountability.
9. Modern management theory and practice focus on achieving desired results with non-blame and non-fear approaches.
10. A culture of control through fear is increasingly inconsistent with expectations in modern democracies.

> **Workplace Deaths**
>
> One of the most dramatic illustrations of the limitations of traditional approaches, and the importance of a focus on outcomes, is a study of workplace fatalities which compared approaches in Germany, France and the UK. The evidence indicated that the highest number of occupational deaths occurred in France despite a high number of inspections and sanctions. The case study showed that there was **no** link between frequent inspections and sanctions and the desired results. By contrast, targeting, differentiation, engagement, and prevention seemed to give the best results. Certainly, the research demonstrated that the "Deterrence" model could not be validated and that focusing on actively **preventing** risks is more productive than "risk-focused deterrence". (See Annex 1 for more detail.)

3. Recent approaches to regulation

Regulation is fundamentally about behaviour. The optimum outcome is to produce acceptable behaviour and to stop unacceptable behaviour.

Although there is no single consensus about "what works best", and the regulatory pendulum swings to and from, a number of key themes can be identified. These include:

- **Regulatory practice—the behaviour of regulators—**is just as important as the content of laws and regulations.
- Aiming for tangible results—**"outcome-based" regulation—is now widely recognised as a high-level regulatory principle.** In other words, any effective regulatory delivery model should focus, as far as possible, on outcomes, going wider than "law enforcement" and resisting pressures to seek compliance for its own sake or to impose excessive regulatory prescription.
- **Effective regulators adopt a risk-based approach**. This means that the supervisory framework, including interpretation and enforcement, is targeted at managing the main risks to the regulatory objectives.
- Effective regulators select the most appropriate approach from a **wide range of compliance-producing tools**, engaging with those they regulate and preferring "voluntary compliance" to enforcement where possible.

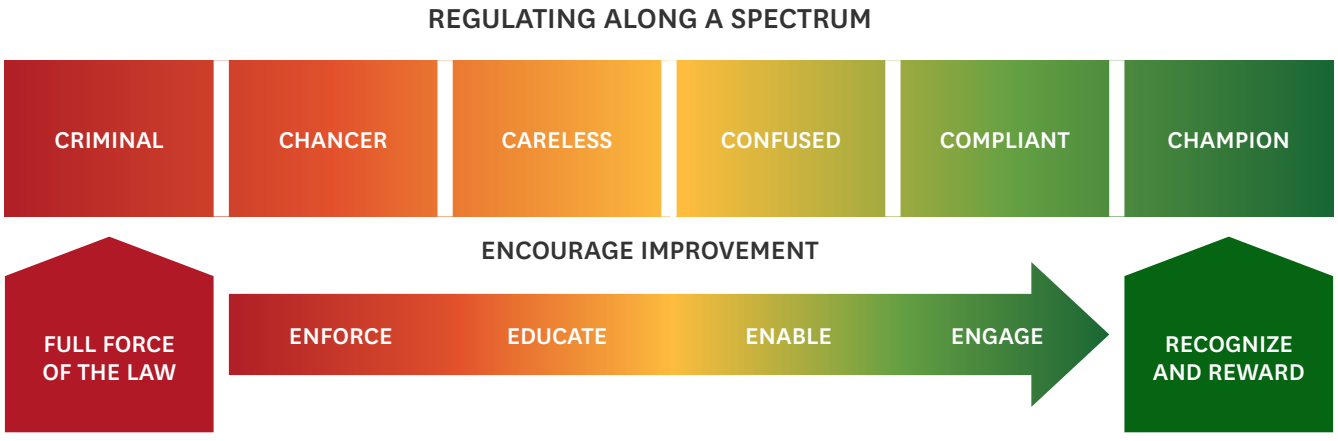
- Regulation alone cannot achieve compliance. Regulators need to exploit a range of levers in addition to their formal powers to ensure that standards are upheld. These levers include the influences which come from users, consumers and citizens (especially where they can make choices in a competitive marketplace and democratic arenas), from peer pressure amongst regulatees, competitor behaviour, conventional and social media comments, and reputational considerations. Organisational accountability and **enlightened self-interest** demonstrated in accountable privacy and data management programmes—where compliance is seen as entirely consistent with increased profitability, improved reputation or fulfilment of other corporate goals—is often a dominant factor.
- Even where regulatory bodies hold significant power to enforce the law, in rule-of-law jurisdictions, they must **act fairly and proportionately, follow due process, and be accountable** for their actions.

4. Segmentation

Moving away from excessive reliance on deterrence and punishment, modern approaches to regulation are based on evidence that the overwhelming majority of businesses do not intend to cause harm or to break the law. When pursuing a focus on achieving desired outcomes through acceptable behaviours, three themes predominate:

1. reserving "conventional" enforcement for serious cases of deliberate, repetitive or cavalier law-breaking;
2. in preference to punishment, changing the behaviour of those who have broken the law to minimise the likelihood of future non-compliance, and (most importantly)
3. preventing breaches by supporting all those seeking to 'get it right'.

In practice, this involves a process of **Segmentation**, positioning organisations, or at least the people who run them, on a Sinners /Saints spectrum. This will then influence the choices of intervention. This is closely aligned with risk-based regulation. It is not possible to segment the entire population of regulatees, and this cannot be applied rigidly. However, a regulator can usually decide the best approach in the light of available evidence about organisations or sectors. Evidence should be available on stated intentions (especially towards fairness and other ethical values) and a positive or negative track record. The nature and extent of an organisation's historical and current conduct will be an influential factor. This is closely linked with Accountability through which an organisation demonstrates (or fails to demonstrate) its values. As with civil aviation (see Annex 1), attitudes to compliance will be an important factor.



(Courtesy of Florentin Blanc & Prof. Campbell Gemmell / Scotland EPA))

5. Responsive Regulation/Regulatory Delivery

Responsive Regulation and Regulatory Delivery are well-documented concepts which share many features of the OBCR model outlined below. A great deal of research now endorses "responsive" regulation, which places emphasis on engagement through information, advice, and support rather than deterrence and punishment. Research has covered a wide range of regulated activities, including occupational health and safety, water pollution, environmental protection, the mining industry, food processing, care for the elderly and civil aviation. In 2014, the OECD issued an important endorsement of approaches on these lines in *Best Practice Principles for Regulatory Policy*

Experience in these and other fields stresses the benefits of a culture where regulators adopt a positive and proactive approach towards ensuring compliance. This involves regulators carrying out their activities in ways that support and help those they regulate to comply. In particular, high priority should be given to ensuring that clear information, guidance and advice are available to help organisations meet their responsibilities. Such support is even more important for SMEs, who, according to research[11], often believe that they are fully compliant until a person they respect (e.g. a regulator or trade association) points out areas of improvement. SMEs then tend to follow the advice.

A successful regulatory authority focuses on responding to the context and circumstances of each regulatee and to outcome measurement, risk-based prioritisation and well-targeted choices of intervention. The core objective of effective regulation is protection from harm, which is best achieved through modifying behaviour so as to reduce risk. This calls for proportionality (based on the nature of the wrong-doing and the harm caused), accountability, consistency, targeting and transparency. It means concentrating on:

- support for regulatees to comply and grow;
- engagement with regulatees;
- the aim of changing behaviours;
- risk assessment to concentrate resources on areas that pose the highest risks;
- emphasis on authoritative and accessible guidance;
- quick identification of persistent or serious offenders.

11 C Hodges, *Outcome-Based Cooperation: in Communities, Organisations, Regulation, and Dispute Resolution* (Hart, 2022), p. 447.

12 Originally developed in I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

6. Outcome-Based Regulation

A more recent framework approach is the Outcome-Based Co-operative Regulation (OBCR) model[13]. This recognises the limitations of conventional regulation, supervision and enforcement and recognises that the goals of regulators and regulatees need not be in conflict. An accountable business does not want to cause harm and will develop risk and control systems which deliver prosperity and protection.[14] The opposite will risk self-harm through reputational and other commercial damage.

The OBCR model is especially well-suited for organisations (the vast majority) seen—or seeking to be seen—in positive terms on the segmentation spectrum. Its key elements are:

1. Clarity about the *purpose(s)* of the regulatory system as a whole and the *outcomes* that are desired—or not desired.

   This will mean identifying and optimising good outcomes for society—normally a balance between *protection* against unacceptable risks and harms and the delivery of *prosperity, innovation, societal benefits*.

2. *Evidence* to establish whether/how outcomes are being achieved.

   Outcomes—different from regulatory outputs—are the results of activities. A focus on rules, breaches and sanctions can easily overlook wider impacts.

3. *Engagement* between all stakeholders at both design and operational levels.

   All key stakeholders—regulators, regulatees, government and consumers—need to be engaged in the achievement of shared purposes and outcomes and in monitoring what is actually being achieved.

4. Trust between stakeholders

   Maximum accountability inherently entails evidence of such accountability or "demonstrability", but businesses are also increasingly keen to proactively demonstrate their trustworthiness, both to the public and to regulators.

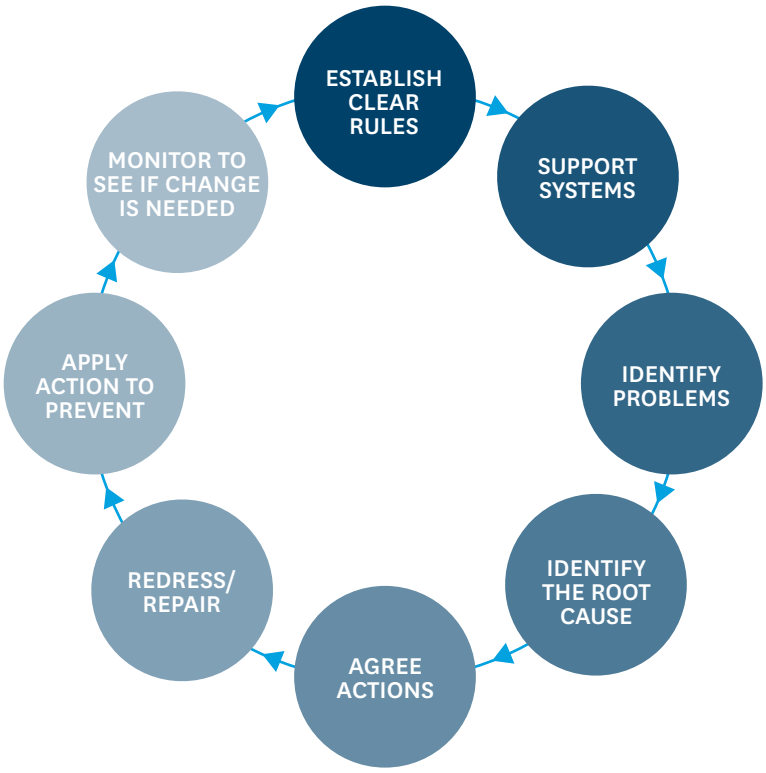
5. Agreement on the appropriate *institutional arrangements*.

   This can include Codes of Practice, innovations such as Sandboxes and commitments to problem-solving and continuous improvement.

13 C Hodges, *Outcome-Based Cooperation: in Communities, Organisations, Regulation, and Dispute Resolution* (Hart, 2022).

14 Centre for Information Policy Leadership, What Good and Effective Data Privacy Accountability Looks Like: Mapping Organizations' Practices to the CIPL Accountability Framework; CIPL White Paper, Organizational Accountability in Data Protection Enforcement - How Regulators Consider Accountability in their Enforcement Decisions.

One particular benefit of this model is the scope it offers for Continuous Performance Improvement[15], which brings together the core functions as follows:



To conclude, modern approaches to regulation focus much more on culture and real-life behaviours. Results are more important than processes. Segmentation helps to identify the "Saints" and the "Sinners" and those on the spectrum between the extremes. Regulators and most regulatees share the same goals. The regulatory burden is reduced. Innovation is encouraged where less importance is attached to prescriptive rules. Ethical behaviour is more likely to be promoted, and a sense of ownership of outcomes within regulated organisations is more likely to be embedded. There is also an incentive to improve performance when regulators are involved in designing models of accountability, assurance, and compliance.

7. Measuring Success

All regulators are accountable for their activities, and almost all will adopt various indicators to measure and demonstrate what and how they are doing. This is an essential component of effectiveness. Performance Indicators which are based on Outputs (as opposed to outcomes) are relatively easy to assemble—for example, the number of investigations conducted, fines imposed or complaints handled. However such indicators have limitations by tending to focus on efficiency and volume, not effectiveness.

Emphasis on outcomes and specific objectives (elaborated in Section IV below) means that regulators need to be increasingly aware of performance indicators which are based on the actual impact of their activities[16]. This is not easy to achieve, especially where the desired results involve improved behaviours. But the task is not impossible. For example, regular surveys

15 Taken from presentation by Prof. Christopher Hodges at 2022 GPA in Istanbul,

16 Chapter 6 of the Global Review of Data Protection Authority Strategies elaborates the case for measures of performance and success, but notes that over half of the DPA strategies reviewed did not include any measurement criteria.

of regulatees' awareness, or use of guidance, will be a measure of effectiveness, especially if they can be used to demonstrate year-on-year improvement. Key Performance Indicators (KPIs) on these lines—widely used in other fields of regulation—will concentrate organisational effort and send powerful signals to all stakeholders.

KEY MESSAGES FROM OTHER SECTORS

- Conventional approaches—adversarial enforcement—have limited effectiveness for changing long-term behaviour within organisations.
- Sanctions are rarely an active deterrent.
- Effective regulators adopt a risk-based approach and focus on behaviours, with choices of intervention guided by segmenting those they regulate.
- Clarity about the desired outcomes is essential.
- Open and constructive engagement, where regulators support trusted regulatees, brings the most benefits.
- Robust penalties should be reserved for deliberate, repeated or wilful wrongdoing.

III. Data Protection is Special

Applying the Messages

Despite the growing consensus about the effectiveness of modern approaches to regulation in other sectors, it may not be straightforward to transfer the key messages to the context of regulating privacy. It can be said, with some justification, that "Data Protection is Special". This is for a number of reasons:

1. No consensus as to the desired outcomes

The starting point for any attempt to measure or improve effectiveness must be clarity about the ultimate outcomes which are being pursued.

In other areas of regulation, the primary outcome will be obvious. The top priority for civil aviation authorities will always be to prevent aircraft crashes. For food safety regulators it will be to stop deaths and serious illnesses.

Privacy and data protection are not absolutes where the primary outcome is obvious. While some may traditionally argue that the primary objective of data protection is the protection of a right to data protection, the question remains: what are the concrete outcomes that need to be achieved to deliver the legislative goal of protecting such a fundamental right? These concepts are elastic and subjective and can also be in tension with other social, economic or political goals and other fundamental rights. The laws tend not to state the intended objective. Often clear consensus within the DPA community as to what outcomes they are trying to achieve is also lacking.

All these factors point to the fundamental conclusion that all DPAs—whether individually or collectively—should work toward articulating and making public the primary outcome they are pursuing. This should be as clear, as succinct and as realistic as possible. It should send clear signals about their priorities and expectations and provide a basis for their own accountability. This fundamental issue is explored further in Section IV.

2. DP laws impact horizontally on all sectors

Data Protection and Privacy laws typically apply widely and universally. They do not usually focus on a particular sector with a well-defined regulated community. They are of comprehensive application and require compliance from private, public, and voluntary sector bodies. There can be few—if any—businesses or other organisations which do not handle personal information. The laws apply to large, medium, small and micro entities, with few allowances for scale or other characteristics. A small organisation can cause damage out of proportion to its size. The application to governments and public bodies can present special sensitivities, especially in any democratic society. Most sectors—such as communications, financial services, and medicine—are subject to simultaneous regulation by other regulators.

This horizontal breadth can also make it difficult for a DPA to know what is actually happening "out there", let alone what technology and other developments lie upstream. DPAs lack reliable insight into the behaviours of those they regulate, in

particular, the reasons why organisations meet or do not meet their legal obligations in relation to data handling. Equally, the inevitable remoteness with such scale brings and makes it hard for regulatees – especially the vast majority who are SMEs—to be aware of and understand their responsibilities. It is thus not at all easy for any DPA to engage or co-operate with regulatees in meaningful ways.

Nevertheless, it is possible to draw upon studies in other regulated areas, and a great deal of anecdotal and other evidence to draw the conclusion that most—though not all—organisations (commercial and governmental) **want** to "get it right". This is driven primarily by recognition of the need for personal information to be handled responsibly. This is manifestly in the interests of the individuals they deal with, whether as consumers, citizens, patients or in some other capacity. But it is also a matter of self-interest, and long-term business sustainability and competitiveness, given the consequences—both reputational and substantive—of getting it wrong.[17]

3. DP laws are complex and focus on procedural compliance

The challenges are compounded by the substance of data protection and privacy laws. Principles are aspirational and expressed in broad and general terms with very few concrete Dos and Don'ts or clarity about what is acceptable or unacceptable. Procedural requirements tend to be prescriptive, complex and convoluted and risk of putting "form over substance". There is no certainty they will produce desired outcomes and there can be disbenefits. Unsurprisingly, there are many uncertainties and disagreements, not least amongst experts.

A "tick-box" approach to compliance with procedural requirements and accountability— often with the help of legal advisers— is relatively easy, but this distracts minds away from the basic aims of the law. It also leads to considerable objections to the "bureaucracy" of data protection and privacy laws, which can translate into questioning of their value.

This can also spread to scepticism amongst the public, who can interpret this bureaucracy as a barrier to the service or benefit they are seeking or, worse still, be told that "data protection" prevents access to what they want. There may even be perverse effects.

> **Privacy Notices: An exercise in futility**
>
> Laws require or encourage Privacy Notices, often with very prescriptive mandatory content. These typically run to thousands of words and attract very poor readability scores. Researchers have found that it would take 76 work days per year for a person to read all of the privacy policies they are confronted with[18].
>
> Consumers, however, are routinely required to confirm that they have read and understood Privacy Notices, which is rarely true. This is neither acceptable nor effective.

4. DP laws set too many functions and no clear priorities

To compound the absence of clear outcomes in the laws themselves, concrete objectives for DPAs are rare, as is any sense of what their priorities should be.

Laws may set out functions, but there is a remarkable lack of legislative guidance as to what DPAs are actually supposed to achieve. At best, the language is general or unrealistic. There is frequent reference to such concepts as "upholding the fundamental rights of individuals", "achieving a high level of data protection", or "ensuring compliance with requirements". But such aspirations can be too hollow without more concrete objectives.

17 Cisco-CIPL Report on *Business Benefits of Investing in Data Privacy Management Programs*, according to the report, 75% of CIPL Members identified "avoiding damage to reputation" as the top three benefits experienced of implementing robust data protection management programmes, p. 9.

18 Privacy Policies Are Difficult to Read.

In the EU, GDPR gives DPAs the broad task of "controlling" or "supervising" the processing of personal data and ensuring compliance with the data protection rules.[19] Article 51 states in very general terms that Supervisory Authorities are "...to be responsible for monitoring the application of this Regulation in order to protect the fundamental rights and freedoms of natural persons..."

Imprecision of specific objectives is exacerbated by the sheer volume of detailed functions. Those set out Articles 57 and 58 of GDPR are a mix of "sticks and carrots"—with some 22 separate "tasks" (where the DPA "shall" undertake the prescribed activity) and 27 powers. These duties and powers appear as a shopping list of 49 items, with no meaningful attempt to prioritise or indicate how they relate to each other. There is no articulation about the overall mission of each DPA. Each function is explicable in isolation, and most are neither controversial nor surprising in themselves. Yet, critically, the GDPR does not set out any "Regulatory Objectives" nor an indication of the overall strategy to be pursued.

5. DPAs are under-resourced

DPAs have pitifully low resources for fulfilling their many responsibilities. This is bound to impact their effectiveness. The recent report on DPA experiences in practice from the EU's Agency for Fundamental Rights[20] confirmed previous findings, which "emphasised that DPAs face difficulties in fulfilling the entirety of their mandate due to a lack of resources." A large majority of (DPA) interviewees stressed that inadequate resources are a "major obstacle to...carrying out the full extent" of their GDPR tasks.

Most DPAs have many new functions and new challenges with the advent of new technologies and the rise of AI. Compared with other regulatory bodies, which typically regulate a much better-defined and much smaller regulated community, DPA resources remain meagre despite any recent increases. Rights and obligations remain aspirational if inadequate resources make them unenforceable or undeliverable.

Governmental funds are the traditional budgetary source for most DPAs. But, with most governments facing economic challenges these are not likely to be significantly increased in the foreseeable future. Moreover, where budgets depend upon governmental funding, the possibility of a threat to independence is increased.

Financing DPAs from the penalties that they impose—beyond the direct legal costs they incur—would equally put in place distorting incentives and be open to ethical and political challenges.

Overall, DPA resources could be increased considerably if fees were to be payable by regulated organisations—as is the norm in many other areas. This approach reduces pressures on public finances and reduces the risks of governmental threats to independence. It also recognises that regulation benefits organisations by increasing public trust and confidence in their activities. It provides a direct channel for engagement between DPA and each organisation. With tiered fees set according to size, substantial income can be administratively simple and cheap to collect. With vast populations of data controllers and processors, such fees could also be kept very modest.

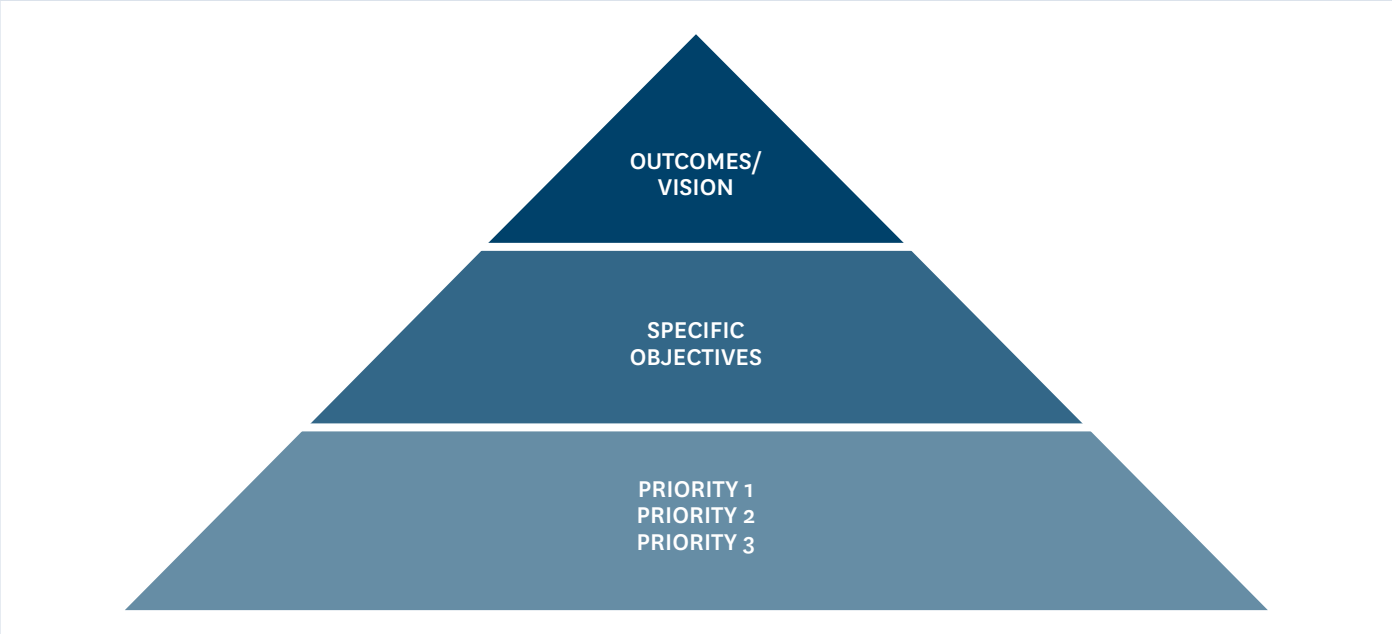
19 Article 16(2) of the Treaty on European Union and Article 8(3) of the Charter of Fundamental Rights.

20 European Union Agency for Fundamental Rights, GDPR in practice – Experiences of data protection authorities.

Data Protection is Special: Key Messages

- The law impacts horizontally on all sectors
- The law is complex and focuses on procedural compliance
- There is no settled consensus as to the desired outcomes
- Laws do not usually give DPAs clear objectives or priorities
- DPAs have too many functions
- They are under-resourced
- Modest fees payable by regulated organisations could considerably increase overall resources

IV. Outcomes, Objectives and Priorities



1. What is everyone trying to achieve?

> **"One of the great mysteries of Data Protection law is the question: *What* is protected?"**[21]

After more than half a century, there remains uncertainty, confusion, or inconsistency about the outcomes that data protection and privacy laws are seeking to produce. This makes it difficult to establish what effectiveness actually means in the context of data protection, let alone any attempt to assess and maximise effectiveness.

It is perhaps not surprising that there is no consensus around optimum outcomes. It reflects that, as noted, privacy is not absolute and is largely subjective. It is dependent upon cultural and contextual factors and has to compete with potentially conflicting rights, freedoms and social or economic goals as reflected in recital 4 GDPR.

Relevant legal instruments lack concrete aspirations and tend to be expressed in abstract terms. Article 8(1) of the EU Charter of Fundamental Rights is circular and is not helpful in this context—"*Everyone has the right to the protection of personal data concerning him or her*." The GDPR lacks a specific purpose, which may reflect the apparent lack of any debate over its

21 Winifried Veil - The Emperor's New Clothes

aims and goals during the European Council, Parliament and trilogue negotiations.[22] The GDPR sets out that the movement of personal data is not to be restricted nor prohibited for reasons of data protection (Art. 1 (3) GDPR), and clarifies that the processing of personal data must serve mankind and the right to data protection is not absolute (Recital 4), but sets out a number of prohibitions with derogations at the same time (Art. 6, 8, 49).[23] This is compounded by a regime of detailed and prescriptive requirements, which—largely without targeting or limitation—apply universally in all sectors.

It is true that a range of rationales for data protection—whether in general or specific provisions—can be identified, some overlapping. However, the variety in itself reinforces concerns about the absence of a primary purpose. Rationales for data protection laws have included:

- upholding fundamental rights and freedoms
- respect for private life
- protection of human dignity
- informational self-determination
- avoidance of discrimination or false inferences
- prevention of financial loss
- avoiding threats to health and safety
- avoiding damage to reputation
- ensuring security of personal data
- securing confidentiality and integrity in IT systems
- maximising free flows of personal data

The most common rationale in European discussion—upholding fundamental rights and freedoms—is abstract, lacks specific context and provides little strategic guidance. It is also silent about how the right to data protection is supposed to interact with other (potentially conflicting and more important) fundamental rights, such as the right to life and freedom of expression, other than the general statement provided in Recital 4 GDPR. It is also significant that the purpose of maximising the free flow of personal data, especially internationally, is often ignored or placed at the end of any list despite it being one of the objectives listed in Art. 1 GDPR.

Opacity and ambiguity about purpose are reflected in the recent Global Review of Data Protection Authority Strategies.[24] This found that 30% of DPAs did not publish any "Vision" at all. The figure rose to 40% of Strategies reviewed in Europe. The authors consider that a vision and mission are "foundational" for any regulatory strategy. "*Without them, there is a risk that more detailed content [of a Strategic Plan], such as objectives, will lack coherence*". The reasons for this silence are not clear. They may reflect the legislative and political reticence or simply be regarded as "too difficult".

Where even some limited vision or mission statements were identified, these include:

- protecting personal data
- upholding privacy rights
- building trust
- promoting transparency
- promoting fundamental rights

22 Ibid. The author was involved in negotiating GDPR for the German government.

23 In German law this is known as "Verbot mit Erlaubnisvorbehalt" – an action is by default prohibited unless a justification is provided by law.

24 Steve Wood, Marie-Charlotte Roques-Bonnet and Sebastian Page, Data Protection Authority Strategies, A Global Review of Current Practice.

- promoting compliance
- empowering citizens.

Most of these echo the abstract rationales noted above and—worthy though they may be in articulating activities—still fail to signal the outcome(s) which are sought. The Global Review also notes that overall, they "*eschew more innovative, digital and tech-focused themes that will be [sic] critical to regulating effectively in the 21st century*."

The absence of clear outcomes has other consequences beyond assessing effectiveness. It impacts any serious attempts to adopt a risk-based approach as foreseen by the GDPR, which cannot succeed unless there is clarity about the potential harms, where "threats" involve the assessment of both the likelihood and gravity of the harms. Likewise, it inhibits any attempt to move towards Accountability for results rather than simply Accountability for compliance. It also makes it more difficult for DPAs to adopt meaningful Key Performance Indicators.

Unsurprisingly, the report come to the conclusion that "[*DPAs] should focus on what it is that they want to be, how they want to be perceived,* **and what their core purpose is**, *rather than where they are today." (Emphasis added).*

In the absence of a clearly defined purpose, it is hard to resist the conclusion that data protection threatens to become an end in itself.

> Uncertainty of purpose amongst DPAs is matched within the regulated community. An ad-hoc survey at CIPL's 2024 Executive Retreat showed an equally wide range of suggestions:
>
> - "An improved and safer existence for every citizen".
> - "Societal & economic benefits from data, with individuals trusting that use".
> - "An effective protection of every individual's right to determine how data about them is being collected and used, whilst also enabling the sharing of data".
> - "Security in Privacy. Stability. Trust Enabler".
> - "Preserve the rights of individuals in relation to data about them and protect people from abuse by the State or other organisations that hold their data, whilst at the same time enabling companies to realise the value of the data they collect and allowing public bodies to use personal data as necessary for the public good".
> - "Individuals exercising agency and control over their data while realising the full societal and economic value that the lawful use of their data has to offer".
> - "Protecting people, society and business".
> - "Put people in control to set and update their own privacy rules".
> - "Eradicate serious, actual harms to data subjects while guaranteeing rights and freedoms of all parties in practice".

2. What should be the Outcome(s)?

It is easier to criticise the absence of purpose than to articulate the "right" outcome(s). Nevertheless, there is a strong case for building an over-arching vision which captures the core outcome that DPAs are seeking to bring about within their statutory powers. Such an exercise will require considerable consultation and debate. It is important that a consensus approach should be primarily articulated and adopted across the DPA community. To be effective, however, the outcome must be supported by all stakeholders and consider all objectives of the law.

Any outcome(s) should be:

- short, concrete and clear;
- visionary and aspirational but realistic;
- easy to elaborate on regulatory objectives and priorities;
- as uncontroversial as possible;
- focussed on the protection of people, not data;
- capable of international and domestic application.

Whether expressed as a Vision, desired Result or Outcome, DPAs need to be able to articulate a strategy and aim against which their activity can be measured . Ideally, there should be a high degree of uniformity—or at least consistency—amongst the (global) community of DPAs in the longer term, while still reflecting the overarching risk-based approach, context of each country and the objectives set by the lawmakers.

These possibilities for the language of explicit outcomes may help to start the debate:

- Ensuring that individuals do not suffer harm from unsafe data use or unacceptable intrusion into their private lives.
- Facilitating the free flow of data with genuine respect for the privacy rights of individuals.
- Ensuring individuals are protected from unexpected or objectionable use of their personal information.
- Minimising the risks arising from the use of personal information.
- Incentivising the responsible use of personal information by organisations

Attempting to capture the key elements of these possibilities, CIPL proposes the following as a suggested Outcome for DPAs to adopt:

> **Facilitating the free flow of data while ensuring that individuals can trust that they will not be significantly harmed by invasions of their privacy or misuse of their personal information.**

3. Regulatory Objectives for DPAs

> **People Protection, not Data Protection**

Once a primary outcome has been articulated, the fundamental for a DPA then is to have clear strategic objectives with a focus on that intended outcome. The outcome becomes the yardstick for setting organisational objectives and signalling how functions are to be prioritised and performed. In other words, what choices of priority are DPAs making to bring about—or at least move towards—the intended outcome?

It is significant, and worrying, that the Global Review of Data Protection Authority Strategies found that a sizeable majority of DPAs—perhaps as many as 65%—appeared not to have a published Strategy at all.

It must be for the leadership of each DPA to adopt a Strategy in order to articulate and communicate—internally and externally—the primary objective(s) it wants to achieve. As a starting point, all effective regulators will ask themselves:

- "What will we be doing to secure the results which we seek?"
- "What does success look like?"
- "How will we know when we've done a good job?"

The Global Review argues that objectives should be SMART—Specific, Measurable Achievable, Realistic and Timely and concluded that the optimal number of objectives appeared to be between three and four.

The legal framework will be relevant in each case, but objectives will need to be expressed in more tangible and realistic language than is usually found in legislation. It is important to avoid generalities, platitudes or vague statements which do not send clear signals. Such concepts as "upholding the fundamental rights of individuals", "achieving a high level of data protection" or "ensuring compliance with requirements" are too hollow to serve as either outcomes or objectives. Objectives need to be concrete and focus on actions.

The basic aim must be geared more towards protecting people in practice, with a wider "social good" dimension. It is also important to go beyond compliance for its own sake. Effective regulation involves monitoring and changing **behaviours** and sometimes cultures, not just ensuring that the formalities and paperwork are in order.

Objectives should therefore not be vague, unrealistic or over-ambitious, but should be consistent with modern thinking about effective regulatory approaches.

It would thus **not** be helpful to adopt such regulatory objectives as:

To deter non-compliance	=	Not sufficiently effective
To punish non-compliance	=	Does not change behaviour in the long run
To ensure the privacy of citizens	=	Too vague
To achieve a high level of data protection	=	Too vague
To uphold fundamental rights and freedoms	=	Too vague
To stop harmful processing of personal data	=	Too ambitious
To supervise the processing of personal data	=	Too vague and not focused on outcomes
To ensure that organisations comply with their obligations	=	Too ambitious and not focused on outcomes
To respond to all complaints	=	Demand-led, resource-intensive and not focused on outcomes

Instead, regulatory objectives should be ambitious, taking into account new developments and the changing nature of society, but as concrete and achievable as possible. They must duly reflect or interpret what the law seeks to achieve and provide a benchmark for the accountability of the DPA's strategy, priorities and actions. Above all, they must signal, internally and externally, what the DPA will actually be doing to bring about the intended outcome.

Each DPA must make its own decisions, and we do not seek to impose our views. Headline objectives flowing from the possible outcomes suggested in the previous section—from which more detailed objectives would then flow—include the following:

Possible Objectives

- We will protect people by promoting responsible use of personal information and ensuring that organisations minimise the risks of individuals.
- We will target unacceptable and harmful uses of personal information which significantly impair the quality of life for individuals or deny them the level of privacy which they can reasonably expect.
- We will adopt a Risk-Based Approach to all our functions – supervision, guidance and enforcement, and focus on areas that present the highest risk and specific harms to individuals.
- We will protect people from unacceptable and harmful use of personal information.
- We will help organisations to understand how to handle personal information responsibly.
- We will maximise the free and safe flow of personal information by incentivising accountable and trustworthy use of data.

4. Strategic Priorities: "Selective to be Effective"

Whatever objectives are adopted, priorities are essential. DPAs cannot do everything.

This is especially important given the typical multiplicity of functions (22 duties and 27 powers in GDPR) and the lack of sufficient resources. It is essential to avoid:

- overwhelmed and ineffective DPAs;
- inadequately protected individuals;
- confused and frustrated regulatees;
- unjustifiable obstacles to the free flow of personal information;
- reputational damage for Data Protection as an obstacle to innovation and societal benefit.

Here, the mantra has to be **"Selective to be Effective"**.

Any well-managed DPA will need to set clear priorities amongst the selected objectives, usually in a transparent Strategic Plan. If priorities are not articulated explicitly, there will still be de facto prioritisation in the shape of work done and work left undone.

What priorities? How should functions (or tasks or activities) be ranked against each other? Using the familiar language of "targeting" or adopting a "risk-based approach" is relatively easy, but much more difficult is going beyond the rhetoric and developing meaningful criteria, principles or other measures to determine the priorities, the targets or the risks which should be tackled.

Despite the typical profusion of functions, nothing in privacy and data protection laws prevents the development of a more strategic, results-based approach. As indicated in Annex 2, it is helpful to group the different **types** of functions into one of three broad types:

1. **Educator ("Leader"):** the functions which rely upon the expertise, authority and support of the DPA;
2. **Enforcer ("Police Officer"):** where enforcement powers are available for breach of a legal requirement;
3. **Complaint-Handler ("Ombudsman"):** where complaints from individuals may seek a remedy.

These grouped functions can then be mapped onto a construct which is familiar to both traditional and modern regulatory approaches:

PREDICT >> PREVENT >> DETECT >> ENFORCE

These are key goals for any regulator, but it is necessary to decide the balance between them and where to place priority. It is not controversial that "Prevent" should be paramount, backed up by "Enforce" when that is necessary. A strategy can then be developed by relating these goals to all the DPA functions.

	LEADER	POLICE OFFICER	OMBUDSMAN
PREDICT	✓		
PREVENT	✓		
DETECT	✓		
ENFORCE	✓	✓	✓

This analysis—and the messages from other regulatory sectors, particularly the need to focus on behaviours and cultures—point very clearly to a broad ranking of priorities in this order:

1. **"Leader"** with emphasis on the expertise, authority and influence of the DPA.
2. **"Police Officer"** where there needs to be enforcement in cases where a requirement may have been breached.
3. **"Ombudsman"** where complaints from individuals demand attention.

Ranking priorities in this way is fundamental if DPAs are to maximise their effectiveness and achieve worthwhile outcomes.

The next three sections examine each of these categories in turn and suggest optimum means of deployment.

OUTCOMES, OBJECTIVES AND PRIORITIES: KEY MESSAGES

- A clear outcome is essential to guide a DPA's objectives and priorities.
- A promising outcome would be to **"Facilitate the free flow of data while ensuring that individuals can trust that they will not be significantly harmed by invasions of their privacy or misuse of their personal information".**
- Objectives should be ambitious but as concrete and achievable as possible.
- Priorities are essential. DPAs have too many functions and cannot do everything.
- In setting priorities, DPAs have to be **"Selective to be Effective".** This means adopting a rigorous risk-based approach in all the activities, from supervision and guidance to regulation, supervision and enforcement, to focus on areas where there is a real likelihood and severity of harm to individuals. This is fundamental if DPAs are to maximise their effectiveness
- The "Leader" role emphasising the expertise, authority and influence of the DPA—should have top priority.
- The "Police Officer" role taking enforcement action—should be ranked in second place.
- The "Ombudsman" role handling complaints from individuals—should have the lowest priority.

V. Leader: To Lead, Educate and Engage

"The guidance that DPAs provide today will produce the results they want tomorrow".

Regulating for Results, CIPL, 2017

"Supporting professionals in their compliance process is one of the CNIL's essential missions.

CNIL Press Release announcing a new Charter, 12 February 2021

The Leadership role should be the top strategic priority for a DPA. It is a role that can only grow in importance in the modern information age. It picks up successful approaches in other regulatory sectors and is directly focused on responsible data handling as the optimum outcome. It cuts across all the goals which need to be fulfilled for maximum effectiveness.

Promoting good practice—the function of educating—lies at the absolute heart of regulatory Leadership. It incentivises and supports improved performance. It embraces those functions which rely upon the expertise and authority of the DPA. An effective DPA will want to be, and be seen to be, the leader in making clear the results and behaviours which it expects the regulated community to achieve or avoid. This involves understanding the technological, commercial and political environments, anticipating issues, interpreting the law and providing guidance that is forward-thinking, practical and strategic. Although they have a part to play here, this is not a role that can be delegated to lawyers, consultants or other advisers, nor left in the hands of regulatees themselves. That is the role of DPAs: to ensure informed, balanced and mature debate about key choices our societies make with respect to privacy and data use, where both interests and rights are equally important.

Guidance must be authoritative, but it must also be usable. It must be in plain language and targeted at identified audiences. Guidance should not create new rules, but provide practical explanations and end examples. The SME community—arguably the most in need—will not read lengthy Opinions, but needs clarity about basic Dos and Don'ts.

The Language of Data Protection

Data Protection has a reputation for being somewhat abstract, almost theological. This is not helped by language. Wherever possible, DPAs should use clear and concrete language in every written communication:

- Target your audience
- Know what you want to achieve
- Keep it short and simple
- Use clear Dos and Don'ts
- Break down long sentences
- Use active verbs, not passive
- Avoid Latin and foreign words
- Test with your audience
- Men, Women, People, Individuals, Consumers, Citizens—**not** Data Subjects
- Information Request—**not** Subject Access Request
- Handling/using information—**not** processing
- Organisation—**not** Data Controller or Data Processor

Guidance must also be proactively and actively distributed and promoted. There are many other players and forces which can be harnessed to promote guidance and the desired regulatory outcomes. Harnessing media and political forces is vital for getting messages across. The pressures of a competitive marketplace, where organisations place enormous value on reputation, likewise need to be fully understood and considered in a strategic approach.

Codes of Practice and certification and seal schemes, whether issued or endorsed by DPAs, can also play an important part in helping organisations get it right. They will invariably be more tangible than pages of legislative text or technical interpretation. Likewise, well-publicised audits can be invaluable in identifying acceptable and unacceptable conduct. This is especially true if they are genuinely designed, executed and promoted as tools which seek to improve, rather than catch out.

1. Constructive Engagement in Practice

All these activities—guidance, codes, audits—carry immeasurable benefits where DPAs **engage** in dialogue with those they regulate and welcome their input. This is especially so where there is a shared common goal of responsible data handling and a common desire to make a practical reality of data protection. DPAs will be able to leverage informed intelligence and know-how from inside regulated organisations—in private and public sectors—to help fulfil their mission.

Segmentation processes will identify the "Champions" where engagement will be the most productive. It requires mutual trust and reinforces the Accountability principle. It is a two-way process—with accountable organisations willing and able to demonstrate their compliance, be transparent about their own activities and share insights into general technological and behavioural trends and innovations. Although leadership must primarily involve dialogue with regulatees, engagement with the public, including civil society, is equally beneficial—or example, through advice, awareness-raising and encouragement of caution and self-help or common events.

A welcome and growing trend towards constructive engagement on the part of some DPAs has already begun, and this can be built upon. Many activities and techniques (both current and prospective) can be identified:

- **Maximum Transparency:** DPAs should be transparent in setting out their priorities, expectations and working methods, which will help DPAs be effective and help organisations to "Get it right the first time". In the same way, organisations must be ready to be transparent when engaging with DPAs without fear or the threat of self-incrimination.
- **Practical Guidance:** Usually web-based, guidance on the interpretation and application of regulatory requirements should, wherever possible, be open for consultation and response by regulated organisations. The best guidance will include plenty of examples and be segmented for maximum ease of use by each target audience—e.g. small businesses, medium enterprises, multinationals, specific business sectors, public bodies, etc.
- **Active Participation:** In open and closed meetings, to communicate both concerns and expectations, participation can be just as important to also find out about uncertainties, trends, commercial and technology developments, etc.
- **Regulated Self-Assurance:** The approach of trustworthy self-compliance places full reliance upon DPOs, codes of conduct, certification schemes, etc., and encourages demonstratable accountability. It can directly reduce pressures on DPAs.
- **Maximum Consultation:** A "No Surprises" approach seeks views on draft guidance or getting feedback on a proposed strategic plan before its final adoption. Such dialogue is especially beneficial when there are new requirements or no common views on what the "right thing" to comply with is or even what should be prevented. A good practice example is the UK Public Consultation Principles, commonly referred to as the Gunning Principles, which are essential for facilitating meaningful dialogue between regulators and regulated entities. According to the principles, four components in conducting public consultation should be considered to make it legitimate:

  1. Consultations must be initiated while proposals are still at a formative stage, meaning decisions have not yet been made.

  2. The information provided to the public should enable respondents to offer informed feedback.

  3. Adequate time must be given for thorough consideration and response, with the UK Government generally recommending a 12-week period for formal consultations.

  4. Decision-makers are obligated to demonstrate that they have carefully considered and taken into account the responses received during the consultation process.

  These principles help ensure transparency, accountability, and public engagement in regulatory decision-making.
- **Frank Exchanges:** There will be benefits from a willingness to participate in confidential discussions, often with a market leader, about the implications and acceptability—or otherwise—of a technological innovation.
- **Sophistication:** DPAs should understand the principles and logic of risk management and compliance policies which seek continuous improvement. They do not use feedback to evidence weaknesses which organisations have openly acknowledged but justifiably treated as low priority. Equally, guidance from DPAs on low-risk or *de minimis* activities is likely to be welcomed as part of a risk-based approach.
- **Exploiting Herd Instinct:** Increasingly, DPAs are recognising that organisations tend to follow a leader of the pack where one or two businesses prominently receive some form of regulatory endorsement or clearance to follow a desirable course of action, competitors, peers, and many others (especially SMEs) will follow the benchmark. There is considerable scope for DPAs to exploit this tendency—promoting best-in-class behaviours, highlighting successful transparency, DPIA and other templates, showcasing best practices of accountable organisations (training or awareness campaigns, DPO leadership, etc.), deliberately influencing key legal and other advisers and highlighting examples of online good practice.

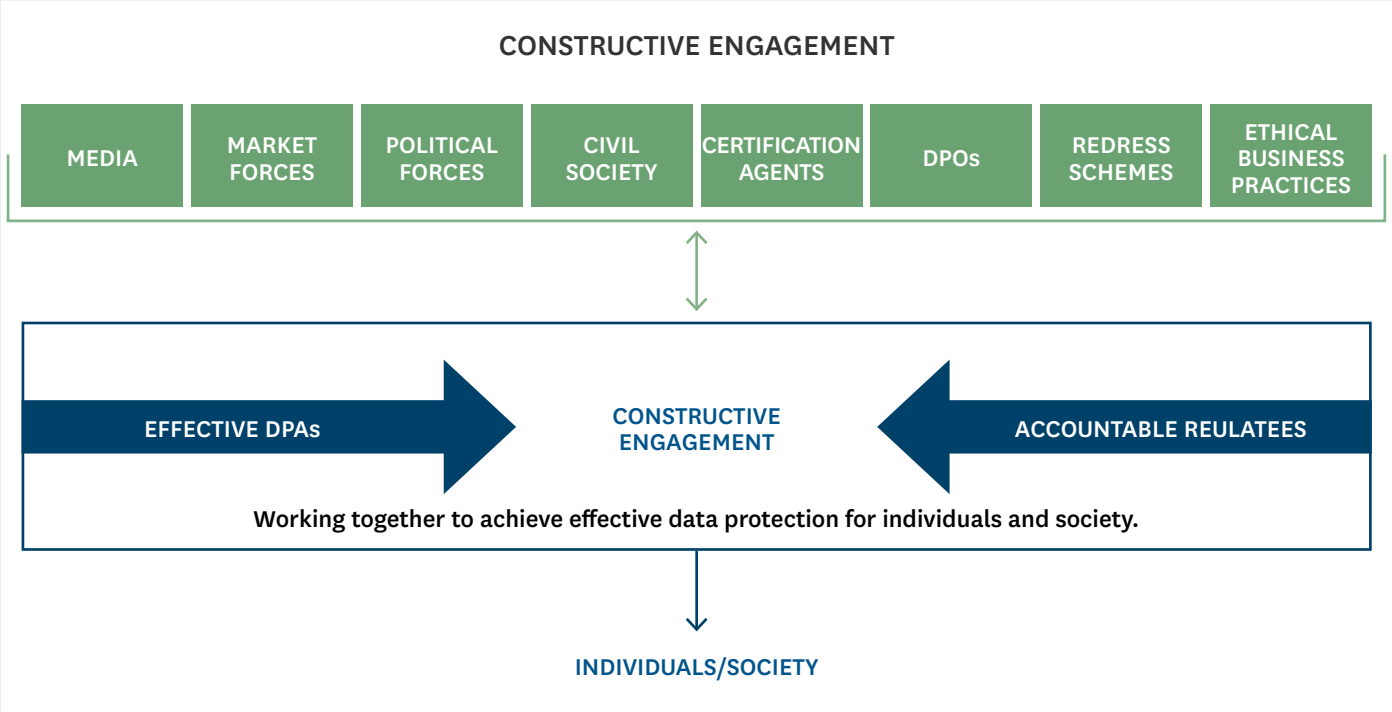
- **Incentives:** Corporate leadership will take data protection and privacy more seriously if DPAs can create and communicate incentives for good faith privacy and compliance programmes. These incentives can include the ability to share data across borders, to engage more broadly in big data and machine learning activities and, crucially, mitigation in case of enforcement.
- **Creating Space for Responsible Innovation:** There is considerable scope for building compliance solutions cooperatively. **Regulatory Sandboxes**—increasingly promoted by DPAs and now enshrined in the EU AI Act—offer one possibility. "Design Thinking", where data privacy requirements and compliance challenges can be made scalable and developed bottom-up by multifunctional teams, may provide other opportunities for regulatory participation and engagement with regulated organisations and experts from other areas (behavioural economists, user-centric designers, technology engineers, marketing and customer relationship experts).
- **Performance Indicators:** Essential for measuring and demonstrating DPA success in directly influencing the spread of good practice, preferably with common and/or comparable metrics.
- **Reiterative guidance and compliance** are going to be necessary to reflect the evolving nature of technology and data uses that data protection law applies to and DPAs seek to regulate. Just like software and technology products are released in stages, over time, patched and improved, the same has to be done with regulatory guidance and organisational compliance. Accountability is a journey, and DPAs should acknowledge that.

Constructive dialogue demands—and gains from—a great deal of trust, commitment and mutual respect between DPAs and accountable organisations. Unless organisations are positive about helping DPAs develop a better understanding of the landscape they regulate, they cannot expect DPAs to be open and comprehending. Regulated businesses and public bodies have to be ready and willing to engage constructively with DPAs. This means coming forward—both proactively and reactively—with an approach which is as open and frank as possible. Business and governmental organisations need to be able to explain and demonstrate their processes and technology solutions as transparently as possible and be ready to explain and demonstrate business models. This is also a matter of **Enlightened Self-Interest** and is especially promising in an environment where more and more responsible entities pride themselves on their accountability measures. Where an obviously innovatory or controversial proposal is being developed, dialogue is particularly valuable for identifying in advance any modifications that will ensure acceptability—far better than the challenge after launch.

"We need regulators to be independent, just as we need judges and referees to be independent. However, independence cannot come at the price of accountability or engagement, and regulators need to keep their fingers on the pulse of the market through interaction with industry and consumers...In a nutshell, regulators must be engaged but not enmeshed, insulated but not insular."[25]

25 'Are regulators the new *Men in Black*?' Cavassini, Naru & Below, in *Risk & Regulation* (LSE, 2016) citing OECD, Being an Independent Regulator.

Constructive engagement can be characterised as creating and operating a framework that captures the contributions of this rich network of stakeholders. This framework diagram illustrates the scope for DPAs to engage directly with regulatees and work with a wide range of other organisations and forces.



LEADERSHIP, EDUCATION AND ENGAGEMENT: KEY MESSAGES

- The Leadership role should be the top strategic priority for a DPA
- Promoting good practice—through the expertise and authority of the DPA—incentivises and supports improved performance.
- Guidance must be authoritative, usable, in plain language and targeted to identified audiences.
- Codes of Practice, certification & seal schemes, and audits can help organisations get it right.
- Constructive engagement with regulatees is the best way to achieve common goals of responsible data handling and make a practical reality of data protection.
- Many activities can be adopted by DPAs wishing to engage constructively.
- Mutual trust—established through segmentation techniques—is an essential component.

VI. Police Officer: To Enforce the Law

The Police Officer's role—investigating, threatening or taking enforcement action against non-compliant organisations—is important and necessary. But it should not be the top priority and should not be the first port of call for any DPA. That would definitely not be the best way to achieve widespread behavioural improvements. The evidence summarised above suggests that such an approach would be both ineffective and possibly counterproductive. The number and size of fines or other punishments are not an indicator of success. Since they apply after the fact, a large number of fines could even be seen as a sign of failure and a lack of behavioural changes.

1. Limitations of Fines and Sanctions

Fines and other sanctions *a priori* or alone do not directly change behaviours. As referenced above,[26] they have a limited effect as a deterrent. Punishing breaches of procedural requirements usually does little to bring about responsible data handling as an outcome. The investigations and evidence-gathering which are essential for successful enforcement are often very costly and divert resources away from more productive activity. Appeals—almost inevitable where substantial fines are imposed—can involve astronomical costs and absorb disproportionate amounts of senior time.[27]

DPAs must always follow a risk-based approach in determining where to focus their enforcement powers: whether to do so in a particular case, what sanctions, and how severe the sanctions should be. The approach must be consistent so that this enforcement action is directed towards real harm, as opposed to a technical breach or DPAs pursuing their own convictions or ideology. Enforcement policy and its practice must be proportionate to the goals sought and harms that DPAs are trying to address.

More generally, reliance upon sanctions takes little or no account of the main drivers of corporate behaviour. Corporate boards do take notice of fines and sanctions. However, in the long run, this is a questionable driver of good behaviour. If the fines become the pace-setters, companies might start to look at data protection as a commercial risk area and make trade-offs. This is not the outcome DPAs or policymakers desire. In reality, companies are increasingly being driven by the long-term need to have a sustainable business that depends on the accountable use of data and the ability to use and share that data responsibly. That includes good data management practices that, as a result, foster digital trust. However, the driving force for good company behaviour should not be based on avoiding fines. Finally, disproportionate fines and sanctions create reticence risk in SMEs and less well-resourced companies, and this is not a desired behaviour where every country is trying to build its own data and AI capabilities and drive competitiveness and economic growth.

Enforcement is inevitably adversarial. There are significant risks that regulatees will adopt defensive, secretive or openly hostile attitudes, which are highly unlikely to improve outcomes for those who are ultimately to be protected. Fines imposed on public bodies are especially problematic.

26 See in particular the work of Prof Hodges as summarised here.

27 [MISSING FOOTNOTE]

None of this is to deny a due role for enforcement. DPAs around the world have been given significantly sharper teeth in recent years. Such sanctions increase credibility and legitimacy and concentrate minds. A profile of strong sanctions shapes perceptions and emphasises the importance of the subject matter. Unfortunately, the media and politicians will mostly associate strong and eye-catching enforcement with effectiveness. All these factors will undoubtedly influence many organisations and may lead to increased resources and top-level attention, especially where commercial or reputational damage is feared.

There is no question that sufficient sanctions must be available or should be used when appropriate. Certain breaches and behaviours—or the failures of other approaches—are so serious that a sanction is inevitable.

Again, the mantra must be "Selective to be Effective." This is where conscious adoption of segmentation techniques on the Sinners/Saints spectrum is helpful. Here, the Accountability principle offers a great deal of scope to separate those who are trustworthy and sincere in their efforts from those who are not. The main targets for enforcement activity (preferably set out as an explicit goal, for example, in an Enforcement Strategy) should be those organisations—the "Sinners"—which are engaging in deliberate, wilful, repeated or cavalier non-compliance with the law.

This approach is entirely consistent with laws which set out factors to be taken into account when deciding whether to fine and/or the amount. These typically include the gravity of the infringement, its intentional or negligent character and any relevant previous infringements. In most cases, some form of warning would be desirable, both to alert the organisation and make it easier for the DPA to show intent or negligence.

2. Enforcement Orders

There is also considerable scope for DPAs to make greater use of powers, which can directly require behavioural changes. Enforcement Orders and similar powers can play a constructive role in securing desired outcomes. They can target an activity which needs to be stopped or changed. They can be used as a mechanism where there are genuine differences of interpretation. They are effective for both private and public sector bodies. They carry weight beyond the recipient organisation.

Enforcement Orders should, however, also not be seen as a first port of call. A change of behaviour which is agreed on a voluntary basis—even with some regulatory arm-twisting—is far more likely to deliver beneficial results than a unilateral imposition. Enforcement Orders should also be seen as an alternative to sanctions wherever possible. They are far less likely to be effective where they are accompanied by a fine or other sanction. That is a recipe for resistance to both measures.[28]

POLICING AND ENFORCEMENT: KEY MESSAGES

- The availability of a meaningful "stick" is important for the credibility and authority of a DPA.
- But enforcement should not be seen as a first resort.
- Fines are not an indicator of success.
- The Police Officer's role and sanctions will be most beneficial against those who have failed to earn trust and whose offending behaviour is deliberate or otherwise unacceptable.
- Enforcement Orders to change behaviour will usually be a preferable remedy.

28 See for example, CIPL White Paper - Organizational Accountability in Light of FTC Consent Orders.

VII. Ombudsman: To Resolve Complaints

Most data protection laws treat a complaint mechanism as an element of the individual's right to data protection. However, it is unusual in other sectors for a regulatory body also to have complaint-handling functions. This recognises that regulating activities and resolving complaints are very different functions.

1. Overwhelmed by Complaints

DPAs can easily be swamped by complaints, as is also evidenced in the recent FRA report.[29] Serious problems and threats to effectiveness will emerge if the Ombudsman role is given excessive priority or not tightly managed. A duty for a regulator to investigate all complaints can easily amount to "Failure by Design". This role is demand-led—almost entirely outside the control of DPAs—and can be very resource-intensive, to the detriment of the other functions. The recent report from the EU Agency for Fundamental Rights noted that the "extremely large and growing" numbers of complaints are a major challenge and should be addressed by DPAs as a priority. It notes that many DPAs are "obliged to prioritise complaints-handling over other regulatory tasks that the GDPR has entrusted to them." Unless cases are handled very carefully, the Ombudsman function can easily distract from more strategic activity. It is very rare for complaints—whether upheld or rejected—to change corporate behaviour. Complainants can be unrepresentative and—despite being high in volume for a DPA—feature a minuscule proportion of the overall population.

Moreover, a significant proportion of complaints are not primarily about data protection. Large numbers of subject access cases involve a dispute with an employer, a bank or public authority on some other issue. The object is to enlist the support of DPA in obtaining information to progress that dispute. In other cases, the individual will simply use the right to complain to pursue a wider grievance against a data controller. As FRA reports, complaints are often repetitive and sometimes petty in nature.[30] The aim of many complainants will often be unachievable, given that the powers of DPAs to award redress are non-existent or very limited.

There are also real risks of creating an environment of public disappointment or disillusionment—whether through backlogs or unwelcome outcomes—and jeopardising the reputation and the popular support which DPAs need. Rather than focusing on relatively few individuals, regulators should therefore concentrate on protecting rights more universally **before** any wrong happens.

Of course, where there is a duty to handle and investigate complaints, the function cannot be ignored altogether. Their main value is as a source of intelligence. An especially serious allegation or a multitude of complaints against the same controller can provide a valuable signal. Sometimes, the subject matter of a complaint will provide valuable "human interest" material for publicising a particular issue. Occasionally, a complaint will reveal a "jewel" with real insight into a new problem.

However well handled, complaints are unlikely to contribute to the desired Outcome. If overall effectiveness is to be achieved by a DPA, ways must be found to ensure that the Ombudsman function has low priority, with complaints handled only to

29 FRA Report notes that: "[DPAs] highlighted how their capacity to supervise the enforcement of the GDPR was jeopardised by the large number of complaints they continue to receive on a regular basis", p. 41.

30 Ibid, p. 20.

the extent appropriate. The FRA report considers grouping of complaints, and the Commission's proposal for harmonised procedural rules for GDPR enforcement proposes the possibility of amicable settlements. Generally, measures that would limit the burden on DPAs by incentivising the parties to engage in complaint handling directly through complaint mechanisms before considering a matter further would go a long way to limit the burden on DPAs and free resources for more impactful tasks.[31]

2. Recalibrating Priority

It will not be easy to give the complaint-handling function a lower priority than other DPA functions. There are, however, various steps that could be taken: DPAs should be explicitly aware that excessive resources used for complaint handling must inevitably reduce overall effectiveness;

- the primary value of complaints as a source of intelligence for identifying risks and harms should be stressed; the complaint-handling role must, therefore, be tightly managed to avoid the swamping of a DPA[32];
- objective criteria should be developed so that as few complaints as possible are investigated in any detail beyond initial acknowledgement and monitoring;
- such criteria could refer to seriousness or impact (to the complainant and to society at large), the motivation and aim of the complainant, the known track record of the organisation and the novelty or consequences of the allegation;
- robust triage arrangements should be introduced to ensure that the criteria are applied swiftly, consistently and fairly;
- enquiries and information requests should be separated from genuine complaints;
- a complaint should be rejected at an early stage without investigation if there is nothing that the DPA could or would do if its allegations were true;
- DPAs should quickly identify excessive, repetitive, abusive, frivolous or vexatious complaints or those which will require disproportionate effort to the expected benefit;
- complainants should be encouraged (or directed) to pursue their grievance through existing Alternative Dispute Resolution (ADR) schemes;
- Certification and seal programmes should encourage such third-party dispute resolution arrangements where possible.

Such measures would alleviate the burdens on DPAs of handling large numbers of complaints that might be better resolved at source or elsewhere. This would enable DPAs to concentrate on more serious or significant complaints.

31 Centre for Information Policy Leadership, Regulating for Results: Strategies and Priorities for Leadership and Engagement, p. 32.

32 It is significant that handling complaints was mentioned as an objective in only 5 of the 51 Strategies reviewed in the Global Review. In practice, however, complaint-handling often takes a disproportionate slice of DPA resources. Available here or a copy can be requested via team@dpa-strategy.org

DPAs should, in any event, publish their policies towards the receipt of complaints. With suitable criteria for investigation, detailed attention can then be reserved, for example, for those complaints which are likely to be strategically valuable. For example, this could embrace those which:

- cumulatively suggest widespread non-compliance affecting many people;
- suggest particularly serious detriment for the complainant;
- allege serious ongoing non-compliance;
- could lead to essential improvements in organisational behaviour;
- raise novel legal, factual or policy issues; or
- suggest that an important point of principle needs to be addressed.

3. Out-sourcing

Although overwhelming numbers of individual complaints have the ability to undermine DPA effectiveness, it does not follow that they are unimportant. Apart from their intelligence value, their authoritative and independent resolution builds consumer and business trust and can be a useful part of the overall infrastructure.

Although the short-term demands lower priority, in the longer term, it should be considered whether the function could be outsourced. A purpose-designed Ombudsman or other ADR body can deliver exactly what is needed, as occurs in other regulated sectors[33]. Consumer Ombudsmen can be very effective at handling small cases, with accessible, low-cost and swift services. Ombudsmen can and must then aggregate microdata and feed it back to the regulator.

There is considerable scope to explore how a satellite Ombudsman service to handle complaints at arms-length for DPAs could be envisioned. Alternatively, the function could be outsourced to an existing ADR-type body, which could add the resolution of data protection complaints to its generalist portfolio.

COMPLAINT-HANDLING: KEY MESSAGES

- Complaint handling is demand-led and very resource-intensive;
- It is unusual for a regulatory body also to handle complaints;
- However well handled, complaints are unlikely to contribute to effectiveness;
- This Ombudsman function should have low priority and be tightly managed to avoid the DPA being swamped;
- Complaints should be treated primarily as a source of intelligence;
- Triage and other mechanisms should be adopted to restrict investigations to cases likely to be strategically valuable.
- DPAs should explore creating a satellite Ombudsman body to handle complaints or out-sourcing to an existing ADR-type service.

33 For example financial services, energy, communications, housing, legal services.

VIII. Overcoming Problems

All strategies involve tough choices. It needs to be openly recognised that any shift of approach brings challenges and risks. Ranking of priorities must mean "losers" as well as "winners". Engagement with regulated organisations may be counter-intuitive and raise genuine worries—both that DPAs may become "captured" and that some regulatees will not welcome excessive DPA involvement in their past, present and future activities. There are, however, several answers to these concerns.

1. Reluctance to Relegate Functions

DPAs themselves will be nervous about downgrading any function which is cast in terms of a statutory duty. Any function which is written as a duty which the DPA "shall" perform cannot be entirely ignored.

Despite the lack of explicit authority, some DPAs already adopted their own high-level values or goals. A transparent and strategic approach is far preferable to ad hoc and unpredictable shifts, driven by events, from one activity to another. Low ranking, or tight management of demand, does not mean abandoning any function in its entirety. Judgement and proportionality are essential. It is increasingly the norm, for example, for other regulatory bodies to give priority to Leadership functions as being more effective in changing behaviours than their Police Officer role. Indeed, it may be inappropriate for any regulator to take enforcement action, seeking to impose severe penalties, for behaviours which it had not previously identified as unacceptable.

Likewise, a general policy of tightly managing complaints in general, but treating only a few as worthy of significant attention is entirely possible. For example, complaints are commonly received and recorded as prima facie evidence of a problem, yet the vast majority may not be subjected to detailed investigation or resolution. The depth of investigation into each complaint is thus proportionate to the potential severity of the matters involved. This requires robust triage arrangements so that the key features of each complaint can be rapidly assessed and (in most cases) complainants can be told why scarce resources and disproportionate efforts cannot be specifically dedicated to them.

2. Regulatory Capture

There may be anxieties about giving greater priority to engagement with regulatees. There may be some concerns about "Regulatory Capture" if DPAs get closer to organisations they regulate. "Regulatory Capture" is described as the process through which the regulated sector can influence and manipulate the agencies that are supposed to control them. This can be seen as a threat to both the independence and integrity of regulators.

Without a doubt, regulators must always properly manage their relationships with those they regulate and limit the risk of "Regulatory Capture". They must be alive to pressures, for example, which could result in improper influence on the selection of "targets" for regulation or enforcement, excessive sympathy with the needs of those they regulate or more lenient penalties. They must equally be alive to the risks of succumbing inappropriately to pressures from increasingly strident advocacy groups.

With maximum transparency and other safeguards, fears of Regulatory Capture should remain largely theoretical. As happens in every field, independent regulators must be able to have an "adult" relationship with those they regulate. This necessitates contact with the regulated sector. A conscious and open "culture of integrity" will help DPAs resist any pressures from the regulated sector. DPAs are rightly proud of their independence and are mature enough to know that independence also means impartiality—looking carefully at both sides of every issue and weighing up all the facts and issues. A corporate culture promoting integrity and high levels of probity will enable DPAs to make the right decisions about appropriate levels of engagement with the regulated sector, both formal and informal.

3. Regulatee Resistance

There may be corresponding concerns from the regulated community that excessive engagement with regulators could be problematic. Some regulated organisations may prefer to keep their distance from a DPA, perhaps because of fear of a penalty for past misconduct, having documents or practices disclosed to the DPA during consultations and then used against them in an enforcement matter, or fear of delays for a planned innovation. This would, however, be equally misguided as a regulator unwilling to engage. Secretive organisations may ironically draw more attention to themselves and it is better to actively seek out advice on new projects in advance rather than discovering it, expensively, at some later stage. Proactive regulators like the UK's ICO and the Ireland DPC offer dedicated services to support this type of engagement. Also, a DPA would risk damage to its own reputation and strategy if it pursued heavy-handed enforcement in response to information disclosed in the course of a supposedly constructive relationship.

More generally, as already stated, engagement is closely connected with organisational accountability and must be a two-way process based on mutual trust. Regulatees cannot expect DPAs to engage constructively unless they also play their part. Part of organisational accountability is precisely to be proactive, transparent, and engage in constructive dialogue with regulators in good faith. Accountable organistions must be expected to do more of this and equally be rewarded by regulators wanting to engage. This is becoming even more essential in the times of transformative technologies and changes to our digital societies and economies. Regulators and regulates, as well as policy and law makers, are all in the same boat and must row together in the same direction.

I. Annex: Experience from other Regulated Sectors

1. Civil Aviation[34]

The regulation of air safety is targeted at corporate culture, behaviour and accountability. Risks are best minimised by open learning from experience. Getting the right outcomes is preferred to compliance with prescriptive regulations. Safety is seen as a joint venture between the regulator and the industry. Matching the cultures of regulators and regulated organisations helps to deliver the right outcomes.

Mandatory occurrence reports were introduced in 1976. Each operator must adopt a *Safety Management System* proportionate to its size and scope. This must include clearly defined lines of responsibility and accountability and the designation of an Accountable Manager. There must be a safety policy understood by all staff and a system for identifying, evaluating and managing all operational hazards.

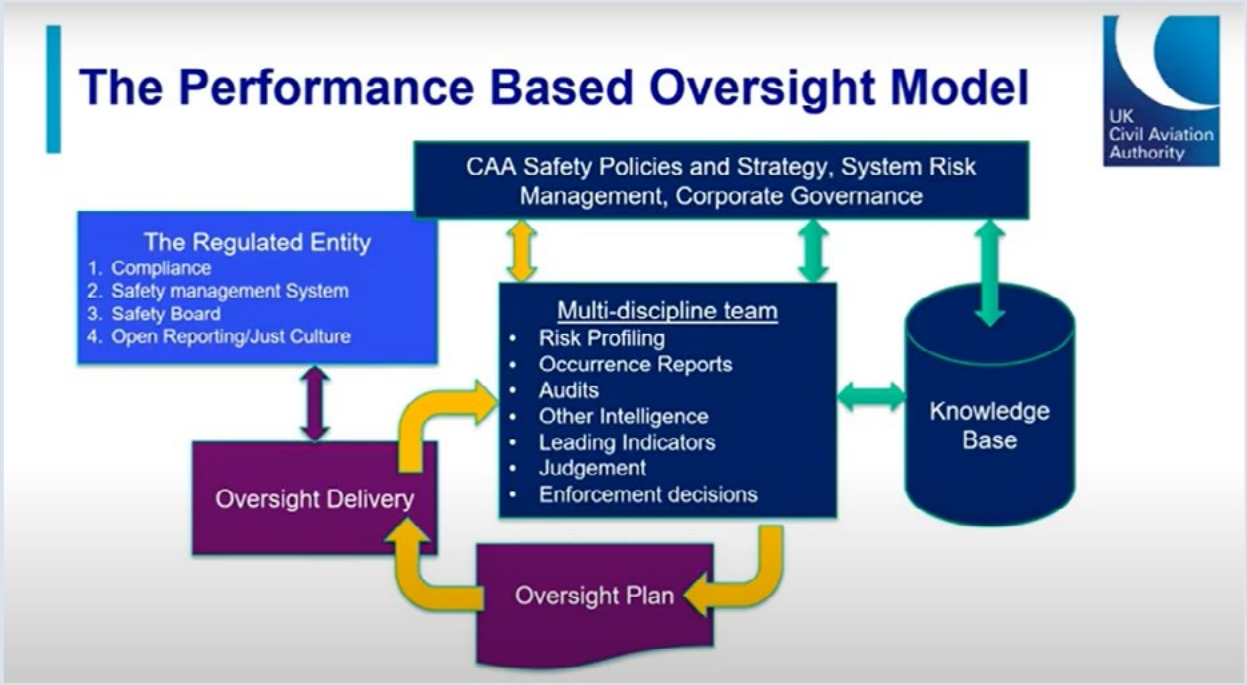
Importance is attached to verifying the effectiveness of actions taken to mitigate risks. A 'Just Culture'—with open reporting—is the bedrock of verification. This means not punishing actions or omissions which are commensurate with experience and training, but not tolerating gross negligence or wilful violations.

The culture of the regulator is equally important in getting desired behaviours from operators. Civil aviation regulators have used dedicated Change Programmes to introduce new processes, new tools and new training. Inspections and audits now focus on risk, shared knowledge and understanding organisational performance. A full understanding of the *attitude* to compliance is a very important part of this, and the design of oversight programmes is based on such intelligence.

'Enforcement' is seen as a broad concept—ranging from advice to drastic intervention. Choosing the right tool is fundamental, and this should be primarily dictated by the changes that the regulator wants to see.

The oversight methodology uses intelligence and data to build and test a risk picture of performance and share that with regulated operators. The basic model can be shown diagrammatically:

34 Summary of presentation by Ben Alcott, International Group Director, Civil Aviation Authority at CIPL seminar in March 2022 which can be viewed here.



2. Workplace Safety: Outcomes, not Compliance

In response to stubbornly high accident rates on construction sites in the 1990s, the UK regulator (the Health & Safety Executive (HSE)) decided on a new approach—to make those involved *own* it as their problem. Instead of inspections on a site-by-site basis across tens of thousands of construction sites, the new approach involved leveraging influence in high-risk areas and engaging and forming partnerships with parties inside the industry able to effect widespread change.

The approach was a significant success. From 2000-2001 to 2012-2013, the number of fatal and major injury accidents fell from 4,410 to 2,161 (49 %).

A study comparing the enforcement policies of various countries with the same laws illustrated clearly that the difference in effectiveness lies not in the rules but in the approach of the authorities.[35] The UK's approach has permanently reduced the occurrence of serious safety incidents. The same approach was followed in Germany, with the same outcome. The approach in France, however, still relies on inspections and penalties for non-compliance with the rules. The "name of the game" is for businesses to pass inspections, not to make workplaces safe. The workplace safety record of France has remained one of the worst in Europe.[36]

3. Financial Services

Fines (and related costs) of well over €350 billion have been imposed on the largest global banks over the past 10 years. Although the "compliance" function has mushroomed, the behaviour of financial institutions has not demonstrably improved.

Regulators of financial services are increasingly recognising the limitation of sanctions as a tool for changing behaviours:

- "The evidence that we have suggests that there are limitations on the extent to which greater compliance can be achieved by increasing fines and the probability of detection" (UK Financial Conduct Authority, 2016)
- "We have learned that simply levying large fines on companies is not enough to create lasting change." (New York Fed, 2019)

35 F Blanc, *From Chasing Violations to Managing Risks. Origins, challenges and evolutions in regulatory inspections* (Edward Elgar).

36 Ibid.

The Regulators are significantly increasing their focus on the causes of misconduct and culture inside institutions:

- The New York Fed uses the language of 'Connect,' 'Convene' and 'Catalyse'
- The Netherlands Central Bank (DNB) has published a book on "Supervision of Behaviour and Culture: Foundations, practice & Future Developments"
- "The law alone cannot compel cultural change." (Central Bank of Ireland)
- "Five Conduct "Questions" - UK Financial Conduct Authority

As part of efforts to establish "a culture of accountability for conduct at the heart of a firm's activities", some jurisdictions have introduced new individual accountability regimes.[37] These aim to clarify who is responsible for what at a senior level and hold senior individuals to account. These include UK (Senior Managers & Certification Regime), Hong Kong (Manager-in-charge regime), Australia (BEAR), Singapore (Guidelines), Ireland (forthcoming SEAR) and Malaysia (forthcoming).

Although there remains a role for sanctions, new individual accountability regimes are primarily aimed at improving governance and behaviours (ultimately through internalisation of norms). They involve clarifying and documenting who is responsible for what at the senior level, codifying conduct standards and requiring senior executives to take "reasonable steps" to ensure compliance.

37. See further, "*New accountability in financial services: Changing individual behaviour and culture*" (J. McGrath, and C. Walker, Palgrave Macmillan 2022)

II. Annex: Classifying DPA Functions under GDPR

In the following table, the main tasks and powers assigned to DPAs have been grouped into three categories.

TASK/POWER	ARTICLE
LEADER	
Promote public awareness of risks, rules, safeguards and rights	57(1)(b)
Promote controller/processor awareness of obligations	57(1)(d)
Advise national parliament, government, etc.	57(1)(c)
Provide information on request to data subjects	57(1)(e)
Monitor the application of Regulation	57(1)(a)
Monitor relevant technologies and commercial practices, etc.	57(1)(i)
Give advice on processing operations requiring a DPIA	57(1)(l)
Encourage and facilitate codes of practice, certification mechanisms and seals & marks	57(1)(m)-(q)
POLICE OFFICER	
Enforce the application of Regulation	57(1)(a)
Conduct investigations on the application of Regulation	57(1)(h)
Order controller/processor to provide information	58(1)(a) & (e)
Obtain access to premises, equipment and means of controller/processor	58(1)(f)
Issue warnings and reprimands	58(2)(a)-(b)
Order compliance	58(2)(c)-(e)
Impose limitations and bans on processing	58(2)(f)
Order rectification, erasure, etc.	58(2)(g)
Impose administrative fines	58(2)(i)
Suspend international data flows	58(2)(j)
COMPLAINT-HANDLER	
Handle and investigate complaints	57(1)(f)

III. Bibliography

This Paper has drawn upon various sources. The following publications are particularly relevant.

Responsive Regulation – Ian Ayres and John Braithwaite, OUP, 1992

A Reader on Regulation – Baldwin, Scott & Hood, OUP, 1998

The Regulatory Craft – Malcolm K. Sparrow, The Brookings Institution, 2000

The Governance of Privacy – Colin Bennett and Charles Raab, MIT Press, 2006

Implementing Hampton: From Enforcement to Compliance – UK Better Regulation Executive, 2006

Really Responsive Regulation – Baldwin & Black – LSE Working Paper, 2007

Risk and Regulatory Policy - Improving the Governance of Risk – OECD, 2010

Regulation, Enforcement and Governance in Environmental Law – Richard Macrory Hart, 2010

Inspection Reform: Why, how & with what Results? – Florentin Blanc, OECD, 2013

Regulators Code – UK Government, 2013

The Governance of Regulators - Best Practice Principles for Regulatory Policy – OECD, 2014

Law and Corporate Behaviour - Integrating theories of regulation, enforcement, compliance and ethics – Christopher Hodges, Hart Publishing, 2015

The European Union as Guardian of Internet Privacy – Hielke Hijmans, Springer, 2016

Regulatory Theory - Foundations and Applications – Peter Drahos, Australian National University, 2017

Regulating for Results – CIPL, 2017

The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society – CIPL, 2018

Incentivising Accountability: How Data Protection Authorities and Law Makers Can Encourage Accountability – CIPL, 2018

Organizational Accountability in Data Protection Enforcement – How Regulators Consider Accountability in their Enforcement Decisions – CIPL, 2021

From Chasing Violations to Managing Risks: Origins, challenges and evolutions in regulatory inspections – Florentin Blanc and Edward Elgar, 2018

Regulatory Delivery – Graham Russell and Christopher Hodges (eds.), Hart Publishing, 2019

Outcome-Based Co-operation in Communities, Business, Regulation and Dispute Resolution – Christopher Hodges, Hart Publishing, 2022

New accountability in financial services: Changing individual behaviour and culture – Joe McGrath and Ciaran Walker, 2022

Global Review of Data Protection Authority Strategies – Steve Wood, Marie-Charlotte Roques-Bonnet and Sebastian Page, 2024

About the Centre for Information Policy Leadership

CIPL is a global data privacy and cybersecurity think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 90 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at

http://www.informationpolicycentre.com/.

DC Office
2200 Pennsylvania Avenue
Washington, DC 20037
+1 202 955 1563

London Office
30 St Mary Axe
London EC3A 8EP
+44 20 7220 5700

Brussels Office
Avenue des Arts 47-49
1000 Brussels
+32 2 643 58 00

24414.0924